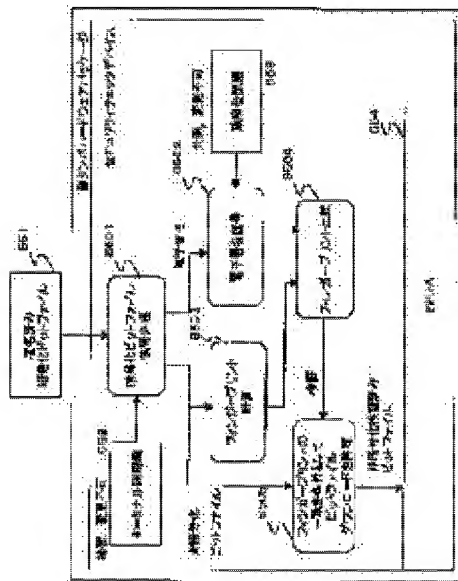D2

PATENT ABSTRACTS OF JAPAN

(11)Publication number :   **2003-122442A**

(43)Date of publication of application : **25.04.2003**

(54) WIRELESS DATA COMMUNICATIONS METHOD AND APPARATUS FOR SOFTWARE DOWNLOAD SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a secure download system of a wireless data communications apparatus.

SOLUTION: Logic that can be reconstructed by a download program and a device for making a security check of the program are stored in a tamper- resistant hardware package of the wireless data communications apparatus. An encryption bit file 551 allows execution of a decryption process by using a terminal secret key 552 (S501). Next, a digital signature (encrypted by use of a hash function) is decrypted by using a government public key 553 that is applicable to all terminals (S502). By application of the hash function, the hash ox fingerprint of the decryption bit file is calculated (S503). If two values are coincident (S504), then software is valid and verified to be unaltered (S505).